33 Legal Ltd

Executive Summary Report

September 2021

Information Commissioner's Office

Background

The Information Commissioner is responsible for enforcing and promoting compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA18), the Privacy and Electronic Communications Regulations (PECR) and other data protection legislation. Section 146 of the DPA18 provides the Information Commissioner's Office (ICO) with the power to conduct compulsory audits through the issue of assessment notices. Section 129 of the DPA18 allows the ICO to carry out consensual audits. The ICO sees auditing as a constructive process with real benefits for controllers and so aims to establish a participative approach.

The ICO's Investigations team ran an investigation between 2017 and 2020 following a number of complaints received from data subjects via the Telephone Preference Service (TPS) and ICO's own online reporting tool. The investigation was focussed on organisations who were making marketing calls using a range of generic and fictitious company names or misusing the names of other genuine companies. By masking their true identity data subjects were prohibited from making complaints directly to these companies and their rights and freedoms provided in data protection legislation were significantly undermined.

33 Legal Ltd (33L) did not form part of the initial investigation; however they were found to be a recipient of personal data obtained as a result of the unlawful collection and compiling of bulk marketing lists. The ICO wrote to 33L in August 2020 outlining their initial concerns, particularly in regard to PECR regulation 21.

33L provided responses to ICO enquiries over a further series of correspondence and also confirmed that they had implemented additional measures, including the appointment of a Head of Compliance to improve their data protection practices.

The ICO wrote to 33L in August 2021 to invite them to take part in a consensual audit. The audit took place during the week beginning 6 September 2021.

The scope of the audit covered the following key control areas:

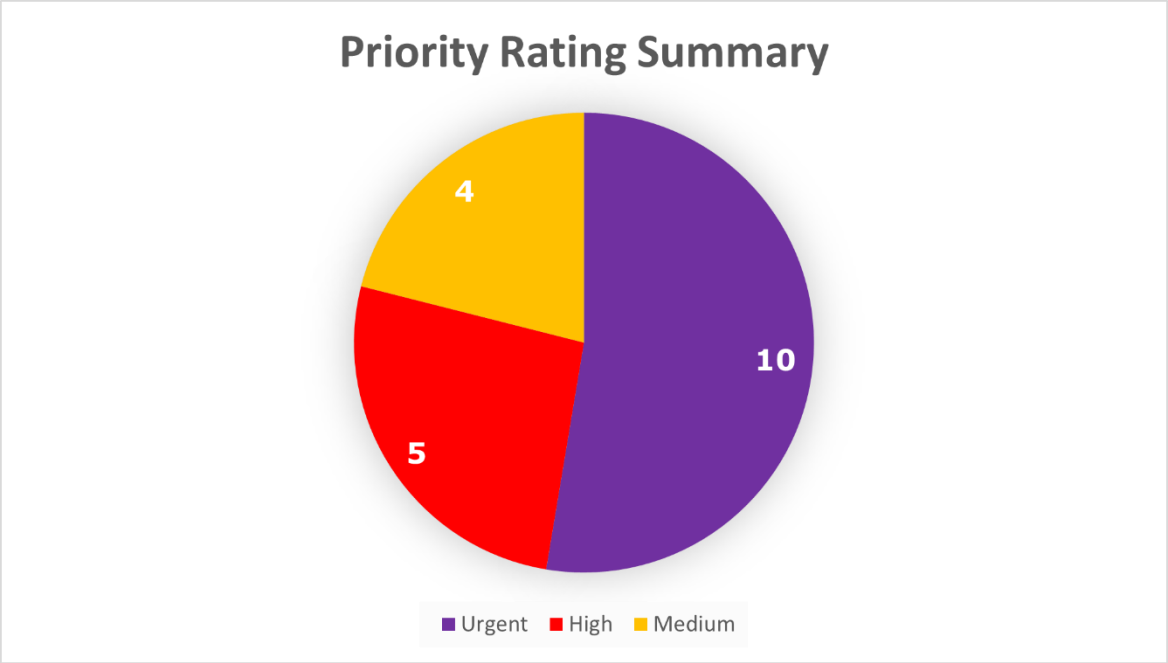
- Governance
- Sourcing personal data
- Transparency
- Lawful basis for processing
- Data supply and sharing

The purpose of the audit was to provide the Information Commissioner with an assurance of the extent to which 33L, within the scope of the audit, is complying with data protection legislation.

Priority of recommendations summary

Where opportunities for improvement were identified recommendations have been made, primarily around enhancing existing processes to facilitate compliance with data protection legislation. In order to assist 33L in implementing the recommendations, each has been assigned a priority rating based upon the risks that they are intended to address. The ratings are assigned based upon the ICO's assessment of the risks involved. 33L's priorities and risk appetite may vary and, therefore, they should undertake their own assessments of the risks identified.

A summary of the ratings assigned within this report is shown below.



The pie chart above shows a breakdown of the priorities assigned to the recommendations made. There are 10 urgent, five high and four medium priority recommendations.

Urgent priority recommendations are intended to address risks which represent clear and immediate risks to 33L's ability to comply with the requirements of data protection legislation.

Areas for Improvement

The ICO are encouraged by the improvements to data protection practices made by 33L since the initial contact in August 2020 including;

- The requirement for all staff to complete annual data protection training.
- The evolution of their business model which limits the processing of personal data to data subjects who have a direct relationship with 33L only.
- The development of a risk based strategy to the processing of personal data including when DPIAs are not required.
- Continuing work towards cyber essentials accreditation.
- Proactive monitoring of internal systems.
- The due diligence process carried out on introducers which provides assurance that 33L can lawfully process personal data.

However, the audit identified some areas where further improvements are required to achieve compliance with data protection legislation.

- There is a limited technical understanding of the UK GDPR. This means that, even where there is a desire to improve and achieve compliance, internal policy and implemented measures may not meet statutory requirements.

- Some contracts in place with introducers and service providers contain out of date information and clauses which do not support compliance with data protection legislation. This means that contracts in place may not be providing the appropriate assurance or protection to 33L or the rights and freedoms of data subjects.

- Published privacy information is not fully compliant with Article 13 of the UK GDPR and is not available to data subjects at the time their personal data are collected.

- 33L have not selected an appropriate lawful basis for some processing activities and others may not have a documented lawful basis. Without appropriate lawful bases 33L will be processing personal data non-compliantly and be unable to provide clear transparency information to data subjects.

- 33L's use of consent as a lawful basis for processing is not compliant with Article 7 of the UK GDPR and therefore undermines the absolute rights afforded to data subjects under this part of the legislation.

Appendices

Appendix One – Recommendation Priority Ratings Description

Urgent Priority Recommendations - These recommendations are intended to address risks which represent clear and immediate risks to the data controller's ability to comply with the requirements of data protection legislation.
High Priority Recommendations - These recommendations address risks which should be tackled at the earliest opportunity to mitigate the chances of a breach of data protection legislation.
Medium Priority Recommendations - These recommendations address medium level risks which can be tackled over a longer timeframe or where some mitigating controls are already in place, but could be enhanced.
Low Priority Recommendations – These recommendations represent enhancements to existing controls to ensure low level risks are fully mitigated or where we are recommending that the data controller sees existing plans through to completion.
